

## О квадратах во множестве элементов конечного поля с ограничениями на коэффициенты при разложении по базису

М. Р. Габдуллин

Усилены недавние результаты C.Dartyge, C.Mauduit, A.Sárközy в задаче о количестве квадратов среди элементов конечного поля с ограничениями на коэффициенты при разложении по базису.

**1. Введение.** При любом фиксированном  $b \in \mathbb{N}$ ,  $b \geq 2$ , каждое число  $n \in \mathbb{N}$  единственным образом представимо в системе счисления с основанием  $b$ :

$$n = \sum_{j=0}^{r-1} c_j b^j, \quad 0 \leq c_j \leq b-1, \quad c_{r-1} \geq 1.$$

Во многих работах (обширный список приведен в [1]) изучались арифметические свойства чисел с "пропущенными" цифрами, т.е. тех чисел,  $b$ -ичная запись которых состоит из заданных цифр.

В [2] С. Dartyge и А. Sárközy рассмотрели аналог этой задачи в конечных полях. Пусть  $\mathbb{F}_q$  — поле из  $q = p^r$  элементов,  $\{a_1, \dots, a_r\}$  — базис  $\mathbb{F}_q$  над  $\mathbb{F}_p$ . Для множества  $\mathcal{D} \subset \mathbb{F}_p$  через  $W_{\mathcal{D}}$  будем обозначать множество элементов поля  $\mathbb{F}_q$ , все коэффициенты которых при разложении по базису  $\{a_1, \dots, a_r\}$  принадлежат множеству  $\mathcal{D}$ . Обозначим через  $Q$  множество ненулевых квадратов поля  $\mathbb{F}_q$ . Положим  $Q_0 = Q \cup \{0\}$ . Будем считать, что  $p \geq 3$ , так как в случае  $p = 2$  мы имеем  $\mathbb{F}_q = Q_0$ .

В недавней работе С. Dartyge, С. Mauduit, А. Sárközy [1] было показано, что если множество  $\mathcal{D}$  достаточно велико, то во множестве  $W_{\mathcal{D}}$  имеются квадраты.

**ТЕОРЕМА А.** Пусть  $\mathcal{D} \subset \mathbb{F}_p$ ,  $2 \leq |\mathcal{D}| \leq p-1$ . Тогда

$$\left| |W_{\mathcal{D}} \cap Q_0| - \frac{|W_{\mathcal{D}}|}{2} \right| \leq \frac{1}{2\sqrt{q}} \left( |\mathcal{D}| + p\sqrt{p-|\mathcal{D}|} \right)^r.$$

Эта оценка нетривиальна, если  $|\mathcal{D}| \geq \frac{(\sqrt{5}-1)p}{2}(1 + o_p(1))$ .

Исследование выполнено за счет гранта Российского научного фонда (проект 14-11-00702).

В случае, когда множество  $\mathcal{D}$  состоит из последовательных чисел, в этой же работе был получен аналог предыдущей теоремы.

**ТЕОРЕМА В.** Пусть  $\mathcal{D} = \{0, \dots, t-1\}$ , где  $2 \leq t \leq p-1$ . Тогда

$$\left| |W_{\mathcal{D}} \cap Q_0| - \frac{|W_{\mathcal{D}}|}{2} \right| \leq \frac{1}{2} (C(p, t) t \sqrt{p})^r,$$

где

$$C(p, t) = \begin{cases} \frac{\log p}{t} + \frac{1}{t} \left( \frac{4}{3} - \frac{\log 3}{2} \right) + \frac{1}{p}, & \text{если } 2 \leq t < p-2, \\ \frac{2}{p} + \frac{2}{\pi(p-1)} (1 - \log(2 \sin \frac{\pi}{2p})), & \text{если } t = p-2. \end{cases}$$

Эта оценка нетривиальна, если  $t \gg \sqrt{p} \log p$ .

В настоящей работе будут доказаны следующие две оценки на количество квадратов во множестве  $W_{\mathcal{D}}$ , из которых вытекает существование квадратов при ограничениях на размер множества  $\mathcal{D}$  более слабых, чем в теореме А.

**Теорема 1.** Пусть  $2r-1 \leq p^{1/2}$ . Тогда справедлива оценка

$$\left| |W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2} \right| \leq \frac{1}{2} |\mathcal{D}|^{1/2} \left( p^{1/4} (2r-1)^{1/2} |\mathcal{D}|^{r-1} + \frac{1}{4} p^{3/4} r^{3/2} + p^{1/2} \right) + \frac{1}{2}.$$

В частности, если  $\delta = (\sqrt{p}(2r-1))^{2-r}$  и  $|\mathcal{D}| \geq (1+\delta)(2r-1)p^{1/2}$ , то  $|W_{\mathcal{D}} \cap Q| \geq 1$ .

**Теорема 2.** При любых натуральных  $\nu$  и  $1 \leq k \leq r-1$  справедлива оценка

$$\left| |W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2} \right| < \frac{1}{2} |\mathcal{D}|^{(r-k)(1-1/2\nu)} \left( (2\nu)^\nu |\mathcal{D}|^{k\nu} q + |\mathcal{D}|^{2k\nu} 4\nu q^{1/2} \right)^{1/2\nu} + \frac{1}{2}.$$

Кроме того, если  $r \geq 20$ ,  $C(r) = \exp\left(\frac{4 \log r + 8}{r}\right) = 1 + o(1)$ ,  $r \rightarrow \infty$ , то при  $|\mathcal{D}| \geq C(r) p^{\frac{1}{2}} \exp\left(\frac{\log p + 4 \log \log p}{r}\right)$  имеем  $|W_{\mathcal{D}} \cap Q| \geq 1$ .

В частности, из теоремы 2 следует, что при большом  $r$  во множестве  $W_{\mathcal{D}}$  есть квадраты уже при  $|\mathcal{D}| > p^{1/2}$ . Отметим, что при  $r \gg \frac{\log p}{\log \log p}$ , более точный результат дает теорема 2, а иначе — теорема 1.

При малых  $r$  теорему В также можно усилить, пользуясь оценкой сумм характеров, полученной в работе С. В. Конягина [3].

**ТЕОРЕМА С.** Пусть  $\varepsilon \in (0, 1/4]$ ,  $\chi$  — нетривиальный мультипликативный характер в  $\mathbb{F}_q$ ,  $N_i, H_i$  — целые числа,  $p^{1/4+\varepsilon} \leq H_i \leq p$ ,  $i = 1, \dots, r$ , и

$$B = \left\{ \sum_{i=1}^r x_i a_i : N_i + 1 \leq x_i \leq N_i + H_i, \quad i = 1, \dots, r \right\}. \quad (1.1)$$

Тогда

$$\left| \sum_{x \in B} \chi(x) \right| \ll \frac{r^{O(1)}}{\varepsilon} p^{-\varepsilon^2/2} |B|.$$

Рассуждая стандартным образом (см., например, начало доказательства теоремы 1), из теоремы С нетрудно вывести следующий результат.

СЛЕДСТВИЕ. Пусть  $\mathcal{D} = \{0, 1, \dots, t-1\}$ ,  $\varepsilon > 0$ ,  $t \geq p^{1/4+\varepsilon}$ . Тогда справедлива оценка

$$\left| |W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2} \right| \ll \frac{r^{O(1)}}{\varepsilon} p^{-\varepsilon^2/2} |W_{\mathcal{D}}|.$$

В частности, если  $\varepsilon \geq C \left( \sqrt{\frac{\log r}{\log p}} + \frac{\log \log p}{(\log p)^{1/2} (\log \log p + \log r)^{1/2}} \right)$  с некоторой абсолютной постоянной  $C > 0$ , то  $|W_{\mathcal{D}} \cap Q| \geq 1$ .

После того, как данная работа была подана в печать, в открытом доступе появилась работа R. Dietmann, C. Elsholtz, I. E. Shparlinski [4], в которой была рассмотрена более общая задача. Пусть  $D_1, \dots, D_r$  – подмножества  $\mathbb{F}_p$ . Положим

$$W = W(D_1, \dots, D_r) = \{x_1 a_1 + \dots + x_r a_r \mid x_i \in D_i\}.$$

Авторы работы [4] отмечают, что доказательство теоремы А [1] переносится на случай, когда множества  $D_i$  различны, а именно, при  $\min_{1 \leq i \leq r} |D_i| \geq \frac{(\sqrt{5}-1)p}{2} (1 + o_p(1))$  справедливо  $|W \cap Q_0| \geq 1$ , и доказывают более сильное утверждение.

ТЕОРЕМА ([4], теорема 3.5). Для любого  $\varepsilon > 0$  существует  $\delta > 0$  такое, что для любых множеств  $D_1, \dots, D_r$ , удовлетворяющих условиям

$$\prod_{i=1}^r |D_i| \geq p^{(1/2+\varepsilon)r^2/(r-1)}$$

и

$$\min_{1 \leq i \leq r} |D_i| \geq p^\varepsilon$$

справедливо  $|W \cap Q_0| = \left(\frac{1}{2} + O(p^{-\delta})\right) |W|$ .

По аналогии с работой [4], теорема В также может быть перенесена на случай различных множеств  $D_i$  (см. [5]).

В разделе 2 мы приводим необходимые вспомогательные результаты. В разделах 3 и 4 приводятся доказательства теорем 1 и 2 соответственно. Далее, в работе [3] множитель  $\frac{r^{O(1)}}{\varepsilon}$  не был выписан явно; для полноты мы докажем теорему С в сформулированном виде в разделе 5.

Автор благодарен С. В. Конягину за постановку задачи и внимание к работе.

**2. Вспомогательные результаты.** Приведём леммы, которые понадобятся нам в дальнейшем.

ЛЕММА D [6],[7]. Пусть  $\chi$  – мультипликативный характер порядка  $s$  в  $\mathbb{F}_q$  и  $\alpha, \beta \in \mathbb{F}_q$  – не сопряжённые порождающие элементы  $\mathbb{F}_q$  над  $\mathbb{F}_p$ . Тогда

$$\left| \sum_{\xi \in \mathbb{F}_p} \chi((\xi + \alpha)(\xi + \beta)^{s-1}) \right| \leq (2r-1)p^{1/2}.$$

ЛЕММА E [8]. Пусть  $t$  – целое число,  $1 \leq t < q$ ,  $\chi_1, \dots, \chi_t$  – мультипликативные характеры в  $F_q$ , причём для некоторого  $i$   $\chi_i \neq \chi_0$ , где  $\chi_0$  – главный характер. Пусть, далее,  $h_1, \dots, h_t$  – различные элементы  $F_q$  и

$$S = \sum_{a \in F_q} \chi_1(a + h_1) \chi_2(a + h_2) \cdots \chi_t(a + h_t).$$

Тогда

$$|S| \leq (t - t_0 - 1)q^{1/2} + t_0 + 1$$

где  $t_0$  – число характеров  $\chi_i$ , для которых  $\chi_i = \chi_0$ .

Хорошо известны оценки сумм характеров по суммам множеств (см., например, [9], лемма 2). Нам будет удобно использовать оценку следующего вида.

ЛЕММА 1. Для любых  $\nu \in \mathbb{N}$ ,  $U, V \subset \mathbb{F}_q$  и квадратичного характера  $\chi$  на  $\mathbb{F}_q$  справедливо

$$\left| \sum_{u \in U} \sum_{v \in V} \chi(u + v) \right| \leq |U|^{1-1/2\nu} \left( \frac{(2\nu)!}{\nu!} |V|^\nu q + |V|^{2\nu} 4\nu q^{1/2} \right)^{1/2\nu}.$$

Док-во. Имеем

$$\left| \sum_{u \in U} \sum_{v \in V} \chi(u + v) \right| \leq \sum_{u \in U} \left| \sum_{v \in V} \chi(u + v) \right| \leq |U|^{1-1/2\nu} S^{1/2\nu},$$

где

$$S = \sum_{u \in U} \left| \sum_{v \in V} \chi(u + v) \right|^{2\nu} \leq \sum_{(v_1, \dots, v_{2\nu}) \in V^{2\nu}} \left| \sum_{a \in \mathbb{F}_q} \chi(a + v_1) \cdots \chi(a + v_{2\nu}) \right|.$$

Последнюю сумму разобьем на две: на сумму  $S_1$  по тем наборам  $(v_1, \dots, v_{2\nu})$ , в которых значение каждой компоненты встречается чётное число раз, и на сумму  $S_2$  по всем остальным наборам. Ясно, что  $S_1 \leq C_{2\nu}^\nu |V|^\nu \nu! q = \frac{(2\nu)!}{\nu!} |V|^\nu q$ . Для оценки внутренней суммы для наборов из суммы  $S_2$  воспользуемся леммой E; каждая полученная оценка будет не больше, чем  $(2\nu - 1)q^{1/2} + 2\nu < 4\nu q^{1/2}$ . Поэтому

$$S \leq S_1 + S_2 < \frac{(2\nu)!}{\nu!} |V|^\nu q + |V|^{2\nu} 4\nu q^{1/2}.$$

Лемма доказана.

**3. Доказательство теоремы 1.** Через  $\chi$  обозначим квадратичный характер на  $\mathbb{F}_q$ ; считаем, что  $\chi(0) = 0$ . Пусть 0 не принадлежит  $\mathcal{D}$ . Тогда

$$|W_{\mathcal{D}} \cap Q| = \frac{1}{2} \sum_{x \in W_{\mathcal{D}}} (1 + \chi(x)) = \frac{1}{2} |W_{\mathcal{D}}| + \frac{1}{2} \sum_{x \in W_{\mathcal{D}}} \chi(x) = \frac{1}{2} |\mathcal{D}|^r + \frac{1}{2} \sum_{x \in W_{\mathcal{D}}} \chi(x).$$

Если же  $0 \in \mathcal{D}$ , то

$$|W_{\mathcal{D}} \cap Q| = \frac{1}{2} \sum_{x \in W_{\mathcal{D}} \setminus \{0\}} (1 + \chi(x)) = \frac{1}{2} (|\mathcal{D}|^r - 1) + \frac{1}{2} \sum_{x \in W_{\mathcal{D}}} \chi(x).$$

Таким образом, всегда справедлива оценка

$$\left| |W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2} \right| \leq \frac{1}{2} \left| \sum_{x \in W_{\mathcal{D}}} \chi(x) \right| + \frac{1}{2}, \quad (3.1)$$

и нужно для доказательства нужно оценить сумму характеров. Положим  $b_j = a_j/a_1$ . Тогда  $b_1 = 1$  и  $\{1, b_2, \dots, b_r\}$  — базис. Имеем

$$\left| \sum_{x \in W_{\mathcal{D}}} \chi(x) \right| \leq \sum_{c_1 \in \mathcal{D}} \left| \sum_{c_2, \dots, c_r \in \mathcal{D}} \chi(c_1 a_1 + \dots + c_r a_r) \right| \leq |\mathcal{D}|^{1/2} A^{1/2}, \quad (3.2)$$

где

$$A = \sum_{c_1 \in \mathcal{D}} \left| \sum_{c_2, \dots, c_r \in \mathcal{D}} \chi(c_1 a_1 + \dots + c_r a_r) \right|^2 = \sum_{c_1 \in \mathcal{D}} \left| \sum_{(c_2, \dots, c_r) \in \mathcal{D}^{r-1}} \chi(c_1 + c_2 b_2 + \dots + c_r b_r) \right|^2.$$

Пусть  $\mathcal{D}_d$  — множество тех наборов  $(c_2, \dots, c_r) \in \mathcal{D}^{r-1}$ , для которых элемент  $c_2 b_2 + \dots + c_r b_r$  лежит в подполе порядка  $p^d$  и не лежит ни в каком подполе меньшего порядка. Ясно, что  $\mathcal{D}^{r-1} = \bigsqcup_{d|r} \mathcal{D}_d$ , причем  $\mathcal{D}_1 = \{0\}$ , если  $0 \in \mathcal{D}$ , и  $\mathcal{D}_1 = \emptyset$  иначе. Для  $d|r$  определим функцию  $f_d(x): \mathcal{D} \rightarrow \mathbb{C}$ ,  $f_d(c) = \sum_{(c_2, \dots, c_r) \in \mathcal{D}_d} \chi(c + c_2 b_2 + \dots + c_r b_r)$ . На-

помним, что  $l_2$ -норма функции  $g: \mathcal{D} \rightarrow \mathbb{C}$  определяется как  $\|g\|_2 = \left( \sum_{x \in \mathcal{D}} |g(x)|^2 \right)^{1/2}$ .

Тогда в силу неравенства треугольника

$$A^{1/2} = \left\| \sum_{d|r} f_d \right\|_2 \leq \sum_{d|r} \|f_d\|_2 = \sum_{d|r} A_d^{1/2}. \quad (3.3)$$

где

$$A_d = \sum_{x \in \mathcal{D}} \left| \sum_{(c_2, \dots, c_r) \in \mathcal{D}_d} \chi(x + c_2 b_2 + \dots + c_r b_r) \right|^2.$$

По определению множества  $\mathcal{D}_d$  при любом  $(c_2, \dots, c_r) \in \mathcal{D}_d$  элемент  $c_2 b_2 + \dots + c_r b_r$  порождает подполе порядка  $p^d$ . Учитывая, что каждый такой элемент имеет не более  $d$  сопряженных, и применяя лемму D к парам несопряженных элементов, при  $d > 1$  имеем

$$A_d \leq \sum_{(c_2, \dots, c_r), (c'_2, \dots, c'_r) \in \mathcal{D}_d} \left| \sum_{x \in F_p} \chi(x + c_2 b_2 + \dots + c_r b_r) \overline{\chi}(x + c'_2 b_2 + \dots + c'_r b_r) \right| \leq \sum_{(c_2, \dots, c_r) \in \mathcal{D}_d} \left( dp + (|\mathcal{D}_d| - d)(2d - 1)p^{1/2} \right) \leq (2d - 1)p^{1/2} |\mathcal{D}_d|^2 + dp |\mathcal{D}_d|.$$

Кроме того,  $A_1 \leq |\mathcal{D}| \leq p$ . Обозначим  $\mathcal{J} = \{d|r : d > 1 \text{ и } \mathcal{D}_d \neq \emptyset\}$ . Тогда при  $d \in \mathcal{J}$  в силу неравенства  $\sqrt{A+B} \leq \sqrt{A} \left(1 + \frac{B}{2A}\right)$ , верного при всех положительных  $A, B$ , получаем

$$A_d^{1/2} \leq (2d - 1)^{1/2} p^{1/4} |\mathcal{D}_d| + \frac{dp^{3/4}}{2(2d - 1)^{1/2}}.$$

Из этой оценки и неравенства (3.3) имеем

$$A^{1/2} \leq p^{1/4} S_1 + \frac{1}{2} p^{3/4} S_2 + p^{1/2},$$

где

$$S_1 = \sum_{d \in \mathcal{J}} (2d-1)^{1/2} |\mathcal{D}_d|, \quad S_2 = \sum_{d \in \mathcal{J}} \frac{d}{(2d-1)^{1/2}}.$$

Учитывая, что  $\sum_{d|r} |\mathcal{D}_d| = |\mathcal{D}|^{r-1}$ , получаем

$$S_1 \leq (2r-1)^{1/2} |\mathcal{D}|^{r-1}, \quad S_2 \leq \sum_{d \in \mathcal{J}} d^{1/2} \leq \frac{1}{2} r^{3/2}.$$

(Последняя оценка проверяется непосредственно при  $2 \leq r \leq 7$ , а при  $r \geq 8$  вытекает из неравенств  $r^{1/2} \leq \frac{1}{6} r^{3/2}$  и  $\sum_{d \leq r/2} d^{1/2} \leq \frac{2}{3} (r/2 + 1)^{3/2} \leq \frac{1}{3} r^{3/2}$ .) Значит,

$$A^{1/2} \leq p^{1/4} (2r-1)^{1/2} |\mathcal{D}|^{r-1} + \frac{1}{4} p^{3/4} r^{3/2} + p^{1/2}.$$

Подставляя последнее неравенство в (3.2), получим

$$\left| \sum_{x \in W_{\mathcal{D}}} \chi(x) \right| \leq |\mathcal{D}|^{1/2} \left( p^{1/4} (2r-1)^{1/2} |\mathcal{D}|^{r-1} + \frac{1}{4} p^{3/4} r^{3/2} + p^{1/2} \right).$$

Отсюда и из (3.1) вытекает первое утверждение теоремы. Далее, во множестве  $W_{\mathcal{D}}$  есть квадраты, если правая часть последнего неравенства  $< |\mathcal{D}|^r - 1$ . Это равносильно условию

$$|\mathcal{D}|^{r-1} \left( |\mathcal{D}|^{1/2} - (2r-1)^{1/2} p^{1/4} \right) > \frac{1}{4} p^{3/4} r^{3/2} + p^{1/2} + |\mathcal{D}|^{-1/2}.$$

Покажем теперь, что последнее неравенство выполнено при  $|\mathcal{D}| \geq (1+\delta)(2r-1)p^{1/2}$ , где  $\delta = (\sqrt{p}(2r-1))^{2-r}$ . В силу того, что  $\sqrt{1+\delta} - 1 \geq \frac{\delta}{2\sqrt{2}}$  при  $\delta \in (0, 1]$ , а также  $2r-1 \geq \frac{3}{2}r$  при  $r \geq 2$ , имеем

$$\begin{aligned} |\mathcal{D}|^{r-1} \left( |\mathcal{D}|^{1/2} - (2r-1)^{1/2} p^{1/4} \right) &\geq (1+\delta)^{r-1} (2r-1)^{r-1/2} (p^{1/2})^{r-1/2} \frac{\delta}{2\sqrt{2}} = \\ &\frac{(1+\delta)^{r-1}}{2\sqrt{2}} (2r-1)^{3/2} p^{3/4} \geq \frac{3\sqrt{3}}{8} p^{3/4} r^{3/2} > \frac{1}{4} p^{3/4} r^{3/2} + p^{1/2} + |\mathcal{D}|^{-1/2}. \end{aligned}$$

Теорема доказана.

**4. Доказательство теоремы 2.** Введём натуральные параметры  $k$  и  $\nu$ , которые выберем позже. Положим

$$U = \left\{ \sum_{j=1}^{r-k} c_j a_j : c_j \in \mathcal{D} \right\}, \quad V = \left\{ \sum_{j=r-k+1}^r c_j a_j : c_j \in \mathcal{D} \right\},$$

где  $1 \leq k \leq r-1$ . Тогда  $W_{\mathcal{D}} = U + V$  и по лемме 1

$$\left| \sum_{x \in W_{\mathcal{D}}} \chi(x) \right| < |\mathcal{D}|^{(r-k)(1-1/2\nu)} \left( (2\nu)^\nu |\mathcal{D}|^{k\nu} q + |\mathcal{D}|^{2k\nu} 4\nu q^{1/2} \right)^{1/2\nu}. \quad (4.1)$$

Отсюда и из (3.1) вытекает первое утверждение теоремы. Далее, положим  $a = |\mathcal{D}|^{-r}$ . Во множестве  $W_{\mathcal{D}}$  есть квадраты, если оценка (4.1) нетривиальна, т.е. если правая часть  $\leq |\mathcal{D}|^r - 1$ . Это равносильно условию

$$(2\nu)^\nu |\mathcal{D}|^{k\nu} q + |\mathcal{D}|^{2k\nu} 4\nu q^{1/2} \leq |\mathcal{D}|^{2k\nu+r-k} (1-a)^{2\nu},$$

или

$$|\mathcal{D}|^{k\nu} \left( |\mathcal{D}|^{r-k} (1-a)^{2\nu} - 4\nu q^{1/2} \right) \geq (2\nu)^\nu q.$$

Пусть  $|\mathcal{D}|^{r-k} \geq 5\nu q^{1/2} (1-a)^{-2\nu}$ , или

$$|\mathcal{D}| \geq (5\nu)^{\frac{1}{r-k}} p^{\frac{r}{2(r-k)}} (1-a)^{-\frac{2\nu}{r-k}} = (5\nu)^{\frac{1}{r-k}} p^{\frac{1}{2} + \frac{k}{2(r-k)}} (1-a)^{-\frac{2\nu}{r-k}} = p^{1/2} \exp \left( \frac{1}{r-k} (\log 5\nu + \frac{1}{2} k \log p + 2\nu \log(1-a)^{-1}) \right). \quad (4.2)$$

Тогда  $|\mathcal{D}|^k \geq (5\nu q^{1/2})^{\frac{k}{r-k}} (1-a)^{-\frac{2\nu k}{r-k}}$  и

$$|\mathcal{D}|^{k\nu} \left( |\mathcal{D}|^{r-k} (1-a)^{2\nu} - 4\nu q^{1/2} \right) \geq \nu q^{1/2} \left( 5\nu q^{1/2} \right)^{\frac{k\nu}{r-k}} (1-a)^{-\frac{2k\nu^2}{r-k}}.$$

Значит, во множестве  $W_{\mathcal{D}}$  имеются квадраты, если выполнено условие (4.2) и неравенство

$$\nu \left( 5\nu q^{1/2} \right)^{\frac{k\nu}{r-k}} (1-a)^{-\frac{2k\nu^2}{r-k}} \geq (2\nu)^\nu q^{1/2}. \quad (4.3)$$

Вместо (4.3) потребуем условие

$$\left( q^{1/2} \right)^{\frac{k\nu}{r-k} - 1} \geq (2\nu)^\nu \quad (4.4)$$

(Так как  $a \in (0, 1)$ , то это условие является более сильным, чем (4.3)). Запишем (4.4) в виде

$$\exp \left( \frac{1}{2} r \log p (k\nu + k - r) \right) \geq \exp ((r-k)\nu \log 2\nu),$$

то есть

$$r \log p (k\nu + k - r) \geq 2\nu(r-k) \log 2\nu,$$

или

$$\log p \left( k + \frac{k}{\nu} - \frac{r}{\nu} \right) \geq 2 \left( 1 - \frac{k}{r} \right) \log 2\nu.$$

Последнее выполнено, если

$$\log p \left( k - \frac{r}{\nu} \right) \geq 2 \log 2\nu,$$

т.е. если

$$k \log p \geq 2 \log 2\nu + \frac{r}{\nu} \log p. \quad (4.5)$$

Таким образом, если выполнены (4.2) и (4.5), то  $|W_{\mathcal{D}} \cap Q| \geq 1$ .

В наших интересах выбрать  $k$  как можно меньше. Минимум в правой части (4.5) достигается при  $\nu = \frac{1}{2}r \log p$ . Положим  $\nu = \lceil \frac{1}{2}r \log p \rceil$ . Тогда для выполнения (4.5) достаточно брать  $k \geq (\log p)^{-1}(2 \log r + 2 \log \log p + 4)$ . Положим

$$k = \left\lceil \frac{2 \log r + 2 \log \log p + 4}{\log p} \right\rceil + 1.$$

Так как при  $u \geq 3$  функция  $\frac{2 \log \log u + 4}{\log u}$  убывает, то  $k \leq \left\lceil \frac{2 \log r + 2 \log \log 3 + 4}{\log 3} \right\rceil + 1 \leq r/2$  при  $r \geq 20$ . Далее, имеем  $\log(1-a)^{-1} \leq \frac{a}{1-a} \leq \frac{4}{3}a = \frac{4}{3}|\mathcal{D}|^{-r} \leq \frac{4}{3}p^{-r/2}$ . Поэтому при выбранных  $\nu$  и  $k$  показатель экспоненты в последней строке (4.2) будет не больше, чем

$$\begin{aligned} \frac{2}{r} \left( \log(5/2) + \log(r \log p) + \log r + \log \log p + 2 + \frac{1}{2} \log p + \frac{4}{3}p^{-r/2}r \log p \right) = \\ \frac{2}{r} \left( 2 \log r + \frac{1}{2} \log p + 2 \log \log p + 2 + \log(5/2) + \frac{4}{3}p^{-r/2}r \log p \right) \leq \\ \frac{1}{r} (4 \log r + \log p + 4 \log \log p + 8). \end{aligned}$$

Отсюда вытекает второе утверждение теоремы.

**5. Доказательство теоремы С.** В этом разделе мы полностью следуем работе [2], лишь отслеживая зависимость констант от параметров  $r$  и  $\varepsilon$ .

**ЛЕММА 2.** Пусть множество  $B$  определено соотношением (1.1), где  $N_i, H_i > 0$  – целые числа, причем  $H_1 = \dots = H_r \leq p^{1/2}$ . Тогда уравнение

$$x^1 x^2 = x^3 x^4, \quad x^1, x^2, x^3, x^4 \in B, \quad (5.1)$$

имеет не более  $r^{O(r)}|B|^2 \log p$  решений.

*Док-во.* Положим  $H = H_1 = \dots = H_r$ ,

$$Z = \frac{B \setminus \{0\}}{B \setminus \{0\}} = \{z \in \mathbb{F}_q : \exists x, y \in B \setminus \{0\} \, xz = y\}.$$

Если  $x^1, x^2, x^3, x^4 \in B$ ,  $x^1 x^2 = x^3 x^4$ , и  $(x^1, x^4) \neq (0, 0)$ ,  $(x^2, x^3) \neq (0, 0)$ , то для некоторого  $z \in Z$  верно  $x^1 z = x^3$ ,  $x^4 z = x^2$ . Поэтому число  $E$  решений уравнения (5.1) оценивается следующим образом:

$$E \leq 2|B|^2 + \sum_{z \in Z} f^2(z),$$

где  $f(z)$  – число решений уравнения

$$xz = y, \quad x, y \in B.$$

Обозначим

$$\begin{aligned} B_0 &= \{x_1 a_1 + \dots + x_r a_r : -H \leq x_j \leq H\}, \\ Z_0 &= \frac{B_0 \setminus \{0\}}{B_0 \setminus \{0\}}, \quad f_0(z) = |\{(x, y) \in B_0^2 : xz = y\}|. \end{aligned}$$



Заметим, что  $f(z) \leq f_0(z)$  и  $f_0(z) = 1$  при  $z \in \mathbb{F}_q^* \setminus Z_0$ . Поэтому

$$\sum_{z \in Z} f^2(z) \leq \sum_{z \in Z_0} f_0^2(z) + |Z \setminus Z_0|.$$

Так как  $|Z| \leq |B|^2$ , получаем

$$E \leq 3|B|^2 + \sum_{z \in Z_0} f_0^2(z), \quad (5.2)$$

и остается оценить последнюю сумму.

Для фиксированного  $z \in Z_0$  определим решетку  $\Gamma$  в  $\mathbb{Z}^{2r}$ :

$$\Gamma = \Gamma_z = \left\{ (x_1, \dots, x_r, y_1, \dots, y_r) \in \mathbb{Z}^{2r} : z \sum_{i=1}^r x_i a_i = \sum_{i=1}^r y_i a_i \right\}.$$

Для фиксированных  $x_1, \dots, x_r \in \mathbb{Z}$  условие  $(x_1, \dots, x_r, y_1, \dots, y_r) \in \Gamma$  определяет вычет по модулю  $p$  каждого из чисел  $y_1, \dots, y_r$ . Значит, количество точек решетки  $\Gamma$  в большом кубе имеет следующую асимптотику при  $M \rightarrow \infty$ :

$$|\{(x_1, \dots, y_r) \in \Gamma : |x_i| \leq M, |y_i| \leq M, i = 1, \dots, r\}| = \frac{(2M)^{2r}}{p^r} (1 + o(1)).$$

Поэтому

$$\text{mes}(\mathbb{R}^{2r}/\Gamma) = p^r. \quad (5.3)$$

Определим куб  $D \subset \mathbb{R}^{2r}$ :

$$D = \{(x_1, \dots, y_r) \in \mathbb{R}^{2r} : |x_i| \leq H, |y_i| \leq H, i = 1, \dots, r\}.$$

Отметим, что

$$f_0(z) = |D \cap \Gamma_z|. \quad (5.4)$$

Напомним, что  $i$ -й последовательный минимум

$$\lambda_i = \lambda_i(z) = \lambda_i(D, \Gamma_z)$$

множества  $D$  по отношению к  $\Gamma_z$  определяется как минимальное число  $\lambda$ , при котором множество  $\lambda D$  содержит  $i$  линейно независимых векторов решетки  $\Gamma_z$ ,  $i = 1, \dots, 2r$ . Очевидно,  $\lambda_1(z) \leq \dots \leq \lambda_{2r}(z)$ , причем условие  $\lambda_1(z) \leq 1$  равносильно тому, что  $z \in Z_0$ . Вторая теорема Минковского (см., например, [6], теорема 3.30) утверждает, что

$$\frac{2^{2r}}{(2r)!} \leq \frac{\lambda_1 \dots \lambda_{2r} \text{mes} D}{\text{mes}(\mathbb{R}^{2r}/\Gamma)}.$$

Учитывая (5.3), получим

$$\lambda_1 \dots \lambda_{2r} \geq \frac{p^r}{(2r)! H^{2r}}. \quad (5.5)$$

Хорошо известно (см. [7], предложение 2.1), что число  $f_0(z)$  точек решетки  $\Gamma$  в кубе  $D$  удовлетворяет неравенству

$$f_0(z) \leq \prod_{i=1}^{2r} \left( \frac{2i}{\lambda_i} + 1 \right) \leq 2^{2r} (2r)! \prod_{i=1}^{2r} \left( \frac{1}{\lambda_i} + \frac{1}{2i} \right) \leq r^{O(r)} \prod_{i=1}^{2r} \max \left( \frac{1}{\lambda_i}, 1 \right). \quad (5.6)$$

Определим полярную решетку  $\Gamma^* = \Gamma_z^*$  как множество векторов  $(u_1, \dots, u_{2r}) \in \mathbb{R}^{2r}$  таких, что

$$\sum_{i=1}^r u_i x_i + \sum_{i=1}^r u_{r+i} y_i \in \mathbb{Z}$$

для всех  $(x_1, \dots, x_r, y_1, \dots, y_r) \in \Gamma$ . Заметим, что  $\Gamma_z^* \subset p^{-1}\mathbb{Z}^{2r}$ , так как  $p\mathbb{Z}^{2r} \subset \Gamma_z$ . Обозначим через  $\lambda_1^* = \lambda_1^*(z)$  первый последовательный минимум решетки  $\Gamma_z^*$  по отношению к множеству

$$D^* = \left\{ (u_1, \dots, u_{2r}) : \sum_{i=1}^{2r} |u_i| \leq \frac{1}{H} \right\}$$

Согласно [8] (см. предложение 3.6), имеем

$$\lambda_{2r} \lambda_1^* \ll r(1 + \log r)^{1/2} = r^{O(1)}. \quad (5.7)$$

Обозначим

$$\nu = \nu(z) = \min \left( \lambda_1 H, \frac{p \lambda_1^*}{H} \right), \quad s = \max \{j : \lambda_j \leq 1\}.$$

Если  $z \in Z_0$ , то  $\lambda_1 \leq 1$  и число  $s$  определено корректно. Заметим также, что  $\nu(z) \geq 1$ .

В случае  $s \leq r$  получаем

$$\prod_{i=1}^{2r} \max \left( 1, \frac{1}{\lambda_i} \right) = \prod_{i=1}^s (\lambda_i)^{-1} \leq (\lambda_1)^{-r} \leq \nu^{-r} H^r.$$

Если же  $s > r$ , то ввиду (5.5) и (5.7) имеем

$$\begin{aligned} \prod_{i=1}^{2r} \max \left( 1, \frac{1}{\lambda_i} \right) &= \prod_{i=1}^s (\lambda_i)^{-1} \leq (\lambda_{2r})^{2r-s} \prod_{i=1}^{2r} (\lambda_i)^{-1} \leq r^{O(r)} (\lambda_1^*)^{s-2r} \prod_{i=1}^{2r} (\lambda_i)^{-1} \leq \\ &= r^{O(r)} \left( \frac{p}{H\nu} \right)^{2r-s} \frac{(2r)! H^{2r}}{p^r} = r^{O(r)} \nu^{-r} H^r \left( \frac{H\nu}{p} \right)^{s-r}. \end{aligned}$$

Но

$$\frac{H\nu}{p} \leq \frac{H^2 \lambda_1}{p} \leq \frac{H^2}{p} \leq 1,$$

и, значит, в обоих случаях справедливо

$$\prod_{i=1}^{2r} \max \left( 1, \frac{1}{\lambda_i} \right) \leq r^{O(r)} \nu^{-r} H^r.$$

Учитывая (5.6), получаем

$$f_0(z) \leq r^{O(r)} \nu(z)^{-r} H^r. \quad (5.8)$$

Положим  $J := [\log_2 H] + 1$  и разобьем множество  $Z_0$  на подмножества  $Z_j$ ,  $j = 1, \dots, J$ , где

$$Z_j = \{z \in Z_0 : 2^{j-1} \leq \nu(z) < 2^j\}.$$

Заметим, что  $Z_j \subset Z_j^1 \cup Z_j^2$ , где

$$Z_j^1 = \{z \in Z_0 : \lambda_1(z)H < 2^j\}, \quad Z_j^2 = \{z \in Z_0 : p\lambda_1^*(z)/H < 2^j\}.$$

Если  $z \in Z_j^1$ , то найдется ненулевой вектор  $v = (v_1, \dots, v_{2r}) \in \Gamma_z$  такой, что  $\max_i |v_i| < 2^j$ . Вектор  $v$  однозначно определяет  $z$ , так как

$$z = \sum_{i=r+1}^{2r} v_i a_{i-r} \left( \sum_{i=1}^r v_i a_i \right)^{-1}.$$

(Случай, когда оба вектора

$$\sum_{i=r+1}^{2r} v_i a_{i-r} \quad \text{и} \quad \sum_{i=1}^r v_i a_i$$

равны нулю в  $\mathbb{F}_{p^r}$  невозможен, так как  $\max_i |v_i| < 2^j \leq p$ ). Поэтому  $|Z_j^1| < (2^{j+1})^{2r}$ .

Аналогично, для  $z \in Z_j^2$  найдется ненулевой вектор  $u = (u_1, \dots, u_{2r}) \in p\Gamma_z^*$  такой, что  $\sum_i |u_i| < 2^j$ . Вектор  $u$  однозначно определяет  $z$ . В самом деле, предположим противное. Тогда найдутся различные  $z'$  и  $z''$  такие, что  $u \in p\Gamma_{z'}^*$  и  $u \in p\Gamma_{z''}^*$ .

Возьмем произвольный элемент  $x \in \mathbb{F}_{p^r}$ ,  $x = \sum_{i=1}^r x_i a_i$ . Пусть

$$y' = xz' = \sum_{i=1}^r y'_i a_i, \quad y'' = xz'' = \sum_{i=1}^r y''_i a_i.$$

Тогда  $(x_1, \dots, x_r, y'_1, \dots, y'_r) \in \Gamma_{z'}$ ,  $(x_1, \dots, x_r, y''_1, \dots, y''_r) \in \Gamma_{z''}$ , и мы имеем

$$\sum_{i=1}^r y_i u_{i+r} \equiv 0 \pmod{p}, \quad (5.9)$$

где  $y_i = y'_i - y''_i$ . Так как уравнение  $xz' - xz'' = y$  разрешимо (относительно  $x$ ) для любого  $y \in \mathbb{F}_{p^r}$ , то сравнение (5.9) выполнено при всех  $(y_1, \dots, y_r) \in \mathbb{Z}^r$ . Значит,

$$u_{r+1} \equiv \dots \equiv u_{2r} \equiv 0 \pmod{p},$$

и в силу того, что  $\max_i |u_i| < 2^j \leq p$ , мы получаем

$$u_{r+1} = \dots = u_{2r} = 0.$$

Отсюда следует, что

$$\sum_{i=1}^r x_i u_i \equiv 0 \pmod{p}$$

при всех  $(x_1, \dots, x_r) \in \mathbb{Z}^r$ , и, стало быть,  $u_1 = \dots = u_{2r} = 0$ , что противоречит выбору вектора  $u$ . Итак, значит, вектор  $u$  однозначно определяет  $z$ , а поэтому  $|Z_j^2| < (2^{j+1})^{2r}$ .

Объединяя полученные выше оценки, имеем

$$|Z_j| \leq |Z_j^1| + |Z_j^2| < 2^{2r+1} 2^{2jr},$$

$$\sum_{z \in Z_j} f_0(z)^2 \leq r^{O(r)} (2^{j-1})^{-2r} H^{2r} |Z_j| \leq r^{O(r)} H^{2r}$$

$$\sum_{z \in Z_0} f_0(z)^2 = \sum_{j=1}^J \sum_{z \in Z_j} f_0(z)^2 \leq r^{O(r)} H^{2r} \log p.$$

Применяя (5.2), получаем утверждение леммы.

Для натурального  $H \leq p/2$  и мультипликативного характера  $\chi$  на  $\mathbb{F}_{p^r}$  положим

$$\Delta(H, \chi) = \max_B \left| \sum_{x \in B} \chi(x) \right| |B|^{-1},$$

где максимум берется по всем параллелепипедам вида (1.1) таким, что

$$H \leq H_i \leq 2H, \quad i = 1, \dots, r. \quad (5.10)$$

Иногда мы будем писать  $\Delta(H)$  вместо  $\Delta(H, \chi)$  для фиксированного характера  $\chi$ . Заметим, что если рёбра параллелепипеда  $B$  удовлетворяют более слабым, чем (5.10), условиям, а именно,

$$H \leq H_i \leq p, \quad i = 1, \dots, r,$$

то его можно разбить на параллелепипеды, рёбра которых удовлетворяют условиям (5.10). Поэтому

$$\left| \sum_{x \in B} \chi(x) \right| \leq \Delta(H, \chi) |B|,$$

и для того, чтобы доказать теорему С, достаточно проверить, что при всех  $0 < \varepsilon \leq 1/4$  справедливо

$$\Delta([p^{1/4+\varepsilon}], \chi) \ll \frac{1}{\varepsilon} r^{O(1)} p^{-\varepsilon^2/2}. \quad (5.11)$$

Приведем еще один вспомогательный результат.

**ЛЕММА 3** [2, лемма 2]. Пусть множество  $B$  определено соотношением (1.1), где  $N_i, H_i > 0$  — целые числа, удовлетворяющие (5.10). Предположим, что  $H, \tilde{H}$  — натуральные числа,  $\tilde{H} \leq H/2$ , и элемент  $u = \sum_{i=1}^r u_i a_i$  удовлетворяет условию

$$1 \leq u_i \leq \tilde{H}, \quad i = 1, \dots, r.$$

Пусть, далее,  $\chi$  — мультипликативный характер в  $\mathbb{F}_{p^r}$ . Тогда

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x+u) \right| \leq 6r \Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H}.$$

Следующая лемма основана на хорошо известном методе, разработанном Бёрджесом (см., например, [9],[10],[11]), который позволяет получить оценку сумм характеров через лемму 2 и лемму Е.

ЛЕММА 4. Пусть  $s, H, \tilde{H}$  — натуральные числа, и

$$G := [p^{r/(2s)}] \leq \tilde{H} \leq \frac{H}{2}, \quad H \leq p^{1/2}.$$

Пусть также  $\chi$  — нетривиальный мультипликативный характер на  $\mathbb{F}_{p^r}$ . Тогда имеет место следующее неравенство:

$$\Delta(H, \chi) \leq 6r\Delta(\tilde{H})\frac{\tilde{H}}{H} + O(sr^{O(r/s)}(\log p)^{1/(2s)}(H\tilde{H}G^{-1}p^{-1/2})^{-r/(2s)}).$$

Док-во. Положим  $I = [1, G] \cap \mathbb{Z}$ ,  $H_0 = [\tilde{H}/G]$ , и

$$B'_0 = \left\{ \sum_{i=1}^r x_i a_i : 1 \leq x_i \leq H_0, i = 1, \dots, r \right\}.$$

Заметим, что любой элемент  $x = yz$ ,  $y \in B'_0$ ,  $z \in I$ , может быть представлен в виде

$$x = \sum_{i=1}^r x_i a_i : \quad 1 \leq x_i \leq \tilde{H}, i = 1, \dots, r.$$

Согласно лемме 3, для всех  $y \in B'_0$ ,  $z \in I$  справедливо

$$\left| \sum_{x \in B} \chi(x + yz) - \sum_{x \in B} \chi(x) \right| \leq 6r\Delta(\tilde{H}, \chi)|B|\frac{\tilde{H}}{H}.$$

Поэтому

$$\left| \sum_{x \in B} \chi(x) - \frac{1}{|B'_0|G} \sum_{x \in B, y \in B'_0, z \in I} \chi(x + yz) \right| \leq 6r\Delta(\tilde{H}, \chi)|B|\frac{\tilde{H}}{H}. \quad (5.12)$$

Далее,

$$\begin{aligned} \left| \sum_{x \in B, y \in B'_0, z \in I} \chi(x + yz) \right| &\leq \sum_{x \in B, y \in B'_0} \left| \sum_{z \in I} \chi(x + yz) \right| \\ &= \sum_{x \in B, y \in B'_0} \left| \sum_{z \in I} \chi(xy^{-1} + z) \right| = \sum_{u \in \mathbb{F}_{p^r}} \omega(u) \left| \sum_{z \in I} \chi(u + z) \right|, \end{aligned}$$

где

$$\omega(u) = \left| \left\{ (x, y) \in B \times B'_0 : \frac{x}{y} = u \right\} \right|.$$

Дважды используя неравенство Гёльдера, получаем

$$\begin{aligned} \left| \sum_{x \in B, y \in B'_0, z \in I} \chi(x + yz) \right| &\leq \\ &\left( \sum_{u \in \mathbb{F}_{p^r}} \omega(u) \right)^{1-1/s} \left( \sum_{u \in \mathbb{F}_{p^r}} \omega(u)^2 \right)^{1/(2s)} \left( \sum_{u \in \mathbb{F}_{p^r}} \left| \sum_{z \in I} \chi(u + z) \right|^{2s} \right)^{1/(2s)}. \quad (5.13) \end{aligned}$$

Очевидно,

$$\sum_{u \in \mathbb{F}_{p^r}} \omega(u) = |B||B'_0|. \quad (5.14)$$

Для того, чтобы оценить сумму  $\sum_{u \in \mathbb{F}_{p^r}} \omega(u)^2$ , введём следующее обозначение: для множества  $A \subset \mathbb{F}_{p^r}$  через  $E(A)$  будем обозначать число решений уравнения

$$x^1 x^2 = x^3 x^4, \quad x^1, x^2, x^3, x^4 \in A.$$

Положим  $B^* = B \setminus \{0\}$ . Имеем

$$\begin{aligned} \sum_{u \in \mathbb{F}_{p^r}} \omega(u)^2 &= \omega(0)^2 + \sum_{u \in \mathbb{F}_{p^r}^*} \omega(u)^2 \\ &= \omega(0)^2 + |\{(x_1, x_2, y_1, y_2) \in B^* \times B^* \times B'_0 \times B'_0 : x_1 y_2 = x_2 y_1\}| \\ &\leq |B'_0|^2 + \sum_{\nu \in \mathbb{F}_{p^r}^*} \left| \left\{ (x_1, x_2) \in B^* \times B^* : \frac{x_1}{x_2} = \nu \right\} \right| \left| \left\{ B'_0 \times B'_0 : \frac{y_1}{y_2} = \nu \right\} \right| \\ &\leq |B'_0|^2 + E(B)^{1/2} E(B'_0)^{1/2}. \end{aligned}$$

Используя лемму 2, и принимая во внимание, что  $|B'_0| \leq |B|$ , получим

$$\sum_{u \in \mathbb{F}_{p^r}} \omega(u)^2 \leq r^{O(r)} |B||B'_0| \log p. \quad (5.15)$$

Далее, мы используем оценку последней суммы в (5.13), полученную в [11]. Для полноты мы воспроизводим здесь доказательство.

$$\begin{aligned} \sum_{u \in \mathbb{F}_{p^r}} \left| \sum_{z \in I} \chi(u+z) \right|^{2s} &= \\ &= \sum_{z_1, \dots, z_{2s} \in I} \left| \sum_{u \in \mathbb{F}_q} \chi((u+z_1) \dots u(u+z_s)(u+z_{s+1})^{q-2} \dots (u+z_{2s})^{q-2}) \right|. \end{aligned}$$

Последняя сумма уже оценивалась нами в частном случае, когда  $\chi$  – квадратичный характер, при доказательстве леммы 1. В общем случае работают аналогичные рассуждения. Мы можем применить лемму Е для тех наборов  $(z_1, \dots, z_{2s})$ , в которых хотя бы один элемент встретился ровно один раз. Для таких наборов получим (см. оценку на сумму )

$$\left| \sum_{u \in \mathbb{F}_q} \chi((u+z_1) \dots u(u+z_s)(u+z_{s+1})^{q-2} \dots (u+z_{2s})^{q-2}) \right| < 4sp^{r/2}.$$

Сумму по наборам  $(z_1, \dots, z_{2s})$ , в которых каждый элемент встретился как минимум дважды, оценим произведением  $p^r$  на количество таких наборов. Так как все элементы  $z_1, \dots, z_{2s}$  лежат в некотором подмножестве множества  $I$ , содержащем  $\min(s, G)$  элементов, и для конкретного такого подмножества есть не более  $s$  способов выбрать

каждый элемент, то количество интересующих нас наборов не превосходит  $G^s s^{2s}$ . Поэтому

$$\sum_{u \in \mathbb{F}_{p^r}} \left| \sum_{z \in I} \chi(u+z) \right|^{2s} \leq G^s s^{2s} p^r + 4s G^{2s} p^{r/2},$$

$$\left( \sum_{u \in \mathbb{F}_{p^r}} \left| \sum_{z \in I} \chi(u+z) \right|^{2s} \right)^{1/(2s)} \leq s G^{1/2} p^{r/(2s)} + 2G p^{r/(4s)}.$$

По определению числа  $G$  имеем

$$\left( \sum_{u \in \mathbb{F}_{p^r}} \left| \sum_{z \in I} \chi(u+z) \right|^{2s} \right)^{1/(2s)} \leq (2s+2) G p^{r/(4s)}. \quad (5.16)$$

Подставляя (5.14)–(5.16) в (5.13), получаем

$$\begin{aligned} \left| \sum_{x \in B, y \in B'_0, z \in I} \chi(x+yz) \right| &\ll s r^{O(r/s)} (|B||B'_0|)^{1-1/(2s)} (\log p)^{1/(2s)} G p^{r/(4s)} \\ &= s r^{O(r/s)} (\log p)^{1/(2s)} |B||B'_0| G (|B||B'_0|)^{-1/(2s)} p^{r/(4s)} \\ &\leq s r^{O(r/s)} (\log p)^{1/(2s)} |B||B'_0| G \left( H \left[ \frac{\tilde{H}}{G} \right] p^{-1/2} \right)^{-r/(2s)} \\ &\leq 2^{r/(2s)} s r^{O(r/s)} (\log p)^{1/(2s)} |B||B'_0| G \left( H \tilde{H} G^{-1} p^{-1/2} \right)^{-r/(2s)}. \end{aligned} \quad (5.17)$$

Из последнего неравенства и (5.12) следует, что

$$\left| \sum_{x \in B} \chi(x) \right| \leq 6r \Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H} + O(s r^{O(r/s)} (\log p)^{1/(2s)} |B| \left( H \tilde{H} G^{-1} p^{-1/2} \right)^{-r/(2s)}).$$

Так как выбор  $B$  был произвольным, то лемма доказана.

Предположим в лемме 4, что

$$s \geq 2r. \quad (5.18)$$

Введем параметр  $\alpha$ , удовлетворяющий условию

$$0 < \alpha \leq \frac{1}{(12r)^2}. \quad (5.19)$$

Предположим также, что

$$0 < \varepsilon \leq \frac{1}{4}, \quad H = [p^{1/4+\varepsilon}]. \quad (5.20)$$

Положим

$$H_i = [\alpha^i H], \quad i \geq 0.$$

Пусть  $I$  – наибольшее целое число такое, что  $H_i \geq G$ , где  $G$  определено в лемме 4. Так как  $H \geq G$  в силу (5.18) и (5.20), то число  $I$  определено корректно.

Применяя лемму 4 к  $H_i$  и  $H_{i+1}$ , мы можем последовательно оценить  $\Delta(H_i)$  через  $\Delta(H_{i+1})$ ,  $i = 0, \dots, I-1$ :

$$\Delta(H_i) \leq 6r\Delta(H_{i+1})\frac{H_{i+1}}{H_i} + O\left(sr^{O(r/s)}(\log p)^{1/(2s)}(H_i H_{i+1} G^{-1} p^{-1/2})^{-r/(2s)}\right).$$

Поэтому

$$\begin{aligned} \Delta(H) &\leq (6r)^I \Delta(H_I) \frac{H_I}{H} + \\ &sr^{O(r/s)}(\log p)^{1/(2s)}(Gp^{1/2})^{r/(2s)} \sum_{i=0}^{I-1} O\left((6r)^i \frac{H_i}{H} (H_i H_{i+1})^{-r/(2s)}\right). \end{aligned} \quad (5.21)$$

Далее,

$$\begin{aligned} (6r)^I \Delta(H_I) \frac{H_I}{H} &\leq (6r)^{\log H / (-\log \alpha)} \frac{H_I}{H} \\ &\leq (6r)^{\log p / (-2 \log \alpha)} \alpha^{-1} \frac{2G}{H} = 2p^{\log(6r) / (-2 \log \alpha)} \alpha^{-1} \frac{G}{H}. \end{aligned} \quad (5.22)$$

Принимая во внимание (5.18) и (5.19), получим

$$\begin{aligned} \sum_{i=0}^{I-1} (6r)^i \frac{H_i}{H} (H_i H_{i+1})^{-r/(2s)} &\leq \sum_{i=0}^{I-1} (6r)^i \alpha^i \left(\frac{H^2 \alpha^{2i+1}}{4}\right)^{-r/(2s)} \\ &\leq 2H^{-r/s} \alpha^{-r/(2s)} \sum_{i=0}^{I-1} (6r)^i \alpha^{i(1-r/s)} \leq 2H^{-r/s} \alpha^{-r/(2s)} \sum_{i=0}^{I-1} (6r)^i \alpha^{i/2} \\ &\leq 2H^{-r/s} \alpha^{-r/(2s)} \sum_{i=0}^{I-1} 2^{-i} \leq 4H^{-r/s} \alpha^{-r/(2s)}. \end{aligned} \quad (5.23)$$

Подставляя (5.22) и (5.23) в (5.21), находим

$$\begin{aligned} \Delta(H) &\leq 2p^{\log 6r / (-2 \log \alpha)} \alpha^{-1} \frac{G}{H} + O\left(sr^{O(r/s)}(\log p)^{1/(2s)}(Gp^{1/2})^{r/(2s)} H^{-r/s} \alpha^{-r/(2s)}\right) \\ &\leq 4p^{\log 6r / (-2 \log \alpha)} \alpha^{-1} p^{r/(2s)-1/4-\varepsilon} + O\left(sr^{O(r/s)}(\log p)^{1/(2s)} \alpha^{-1} p^{-(r/s)(\varepsilon-r/(4s))}\right). \end{aligned} \quad (5.24)$$

Для завершения доказательства теоремы С выберем параметры  $s$  и  $\alpha$  следующим образом:

$$s = \left\lceil \frac{r}{2\varepsilon} \right\rceil + 1, \quad \alpha = (6r)^{-3}.$$

Легко видеть, что при этом условия (5.18) и (5.19) выполнены. Так как

$$\frac{4\varepsilon}{3} \leq \frac{r}{s} \leq 2\varepsilon,$$

то

$$\frac{r}{s} \left( \varepsilon - \frac{r}{4s} \right) \geq \frac{2}{3} \varepsilon^2;$$



следовательно,

$$\begin{aligned} (\log p)^{1/(2s)} \alpha^{-1} p^{-(r/s)(\varepsilon-r/(4s))} &\leq (6r)^3 (\log p)^{\varepsilon/r} p^{-2\varepsilon^2/3} \\ &= (6r)^3 \exp\left(\frac{\varepsilon}{r} \log \log p - \frac{\varepsilon^2}{6} \log p\right) p^{-\frac{\varepsilon^2}{2}} \ll r^3 p^{-\frac{\varepsilon^2}{2}}. \end{aligned}$$

Наконец,

$$p^{\log 6r/(-2 \log \alpha)} \alpha^{-1} p^{r/(2s)-1/4-\varepsilon} \leq (6r)^3 p^{1/6} p^{-1/4} \ll r^3 p^{-1/12}.$$

Значит, неравенство (5.24) дает нам

$$\Delta(H) \ll r^3 p^{-1/12} + \frac{r}{\varepsilon} r^{3+O(\varepsilon)} p^{-\varepsilon^2/2} \leq \frac{r^{4+O(\varepsilon)} p^{-\varepsilon^2/2}}{\varepsilon}.$$

Таким образом, неравенство (5.24) влечет неравенство (5.11), и теорема C доказана.

## СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] C. Dartyge, C. Mauduit, A. Sárközy, “Polynomial values and generators with missing digits in finite fields”, **52.1**, *Functiones et Approximatio*, 2015, 65–74.
- [2] C. Dartyge, A. Sárközy, “The sum of digits function in the finite field.”, **141.12**, *Proc. Amer. Math. Soc.*, 2013, 4119–4124.
- [3] S. V. Konyagin, “Estimates of character sums in finite fields”, **88**, **№4**, *Mathematical Notes*, 2010, 503–515.
- [4] Dietmann R, Elsholtz C., Shparlinski I. E., “Prescribing the binary digits of squarefree numbers and quadratic residues.”, arXiv: 1601.04754v1.
- [5] М. Р. Габдуллин, “О квадратах в специальных множествах конечного поля”, [подана в печать].
- [6] A. Winterhof, “Characters sums, primitive elements, and powers in finite fields”, **91**, *Journal of Number Theory*, 2001, 153–161.
- [7] D. Wan, “Generators and irreducible polynomials over finite fields.”, **66**, *Math. Comp.*, 1997, 1195 - 1212..
- [8] J. Johnsen, “On the distribution of powers in finite fields”, **251**, *J. Reine Angew. Math.*, 1971, 10–19.
- [9] S. R. Blackburn, S. V. Konyagin, I. E. Shparlinski, “Counting additive decompositions of quadratic residues in finite fields”, **52.2**, *Functiones et Approximatio*, 2015, 223–227.
- [10] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge Press, 2006.
- [11] U. Betke, M. Henk, J. M. Wills, “Successive-minima-type inequalities”, **9**, *Discrete and computational geometry*, 1993, 165–175.
- [12] W. Banaszczyk, “Inequalities for convex bodies and polar reciprocal lattices in  $R^n$ ”, **13**, *Discrete and computational geometry*, 1995, 217–231.
- [13] D. A. Burgess, “On character sums and primitive roots”, **12**, *Proc. Lond. Math. Soc. (3)*, 1962, 179–192.
- [14] A. A. Karatsuba, “On estimates of character sums”, **4**, *Math. USSR-Izv.*, 1970, 19–29.

- [15] M.-Ch. Chang, “Burgess inequality in  $\mathbb{F}_{p^2}$ ”, **19**, Geom. Funct. Anal., 2009, 1001-1016.

**М. Р. Габдуллин**

Московский государственный университет им.  
Ломоносова

Институт математики и механики УрО РАН.

*E-mail:* Gabdullin.Mikhail@ya.ru

Поступило

00.00.0000